MICHAEL BAILEY
United States Attorney
District of Arizona

KEVIN M. RAPP (Ariz. Bar No. 014249, kevin.rapp@usdoj.gov)
MARGARET PERLMETER (Ariz. Bar No. 024805, margaret.perlmeter@usdoj.gov)
PETER S. KOZINETS (Ariz. Bar No. 019856, peter.kozinets@usdoj.gov)
ANDREW C. STONE (Ariz. Bar No. 026543, andrew.stone@usdoj.gov)
JOHN J. KUCERA (Cal. Bar No. 274184, john.kucera@usdoj.gov)
Assistant U.S. Attorneys
40 N. Central Avenue, Suite 1800
Phoenix, Arizona 85004-4408
Telephone (602) 514-7500

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division, U.S. Department of Justice

REGINALD E. JONES (Miss. Bar No. 102806, reginald.jones4@usdoj.gov)
Senior Trial Attorney, U.S. Department of Justice
Child Exploitation and Obscenity Section
950 Pennsylvania Ave N.W., Room 2116
Washington, D.C. 20530
Telephone (202) 616-2807
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

| | |
|---|---|
| United States of America,<br>Plaintiff,<br>v.<br>Michael Lacey, et al.,<br>Defendants. | CR-18-422-PHX-SMB<br>**UNITED STATES' NOTICE REGARDING STATUS OF BACKPAGE SERVERS, JENCKS, AND PROPOSED DATES FOR EXTENSION OF EXISTING DEADLINES IN THE SCHEDULING ORDER AND PROPOSED ORDER** |

## I. Government's Notice Regarding Status of Backpage Servers, *Jencks*, and Proposed Dates for Extension of Existing Deadlines in the Scheduling Order

On April 23, 2019, the Court conducted a status conference where, among other things, Status Reports (CR, 524, 527, and 528) were discussed. During the status conference, the Court denied Defendants oral motion for the Court to reconsider the disclosure of *Jencks* material as it relates to Carl Ferrer. (*See* Minute Entry for Status Conference on April 23; CR 545). The Court also denied Defendants oral motion to extend the existing deadlines in the Scheduling Order without prejudice. *Id*. Additionally, the Court ordered the government and Defendants to file a notice with the court on the status of the servers, *Jencks*, and proposed dates for extension of existing deadlines in the Scheduling Order. *Id*. [1]

## II. Status of Servers

On March 6, 2019, the government provided Defendants a detailed summary of how it handled of the Backpage server data. (*See* CR 524; Exhibit H). As articulated in that summary, the government currently has 46 servers in its possession obtained from Amsterdam, Netherlands, Tucson, Arizona, and Dallas, Texas. The government will retrieve the remaining servers from Amsterdam (which will include the Backpage Payment Processing Island) the week of June 10, 2019.

### A. Backpage.com Website Servers, DesertNet and W.G.

Since the April 23, 2019, status conference, the government has worked diligently with W.G., Chief Technology Officer for DesertNet (a technology consultant company that handled the administration of the Backpage.com website servers since its inception) to provide specific descriptions and roles of the Backpage.com website servers. (*See* Declaration of IRS Special Agent Richard Robinson, Exhibit D and Attachment 1 to the

[1] During the April 23, 2019, status conference the government also agreed to provide Bates numbers to the exhibits on its preliminary exhibit list to defense counsel. On May 29, 2019, the government provided defense counsel (including David Eisenberg and Joy Bertrand) with Bates numbers for approximately 90% of exhibits contained on its preliminary exhibit list. (*See* Exhibit A). The government will continue to periodically provide Defendants with updated and revised preliminary exhibit list in the coming weeks, to include adding Bates numbers to the approximately 10% of documents that do not already contain them. *Id*. Additionally, on or about May 20, 2019, the government provided counsel Eisenberg and Bertrand with two DVD's. The first DVD contained "hot docs" specifically related to the allegations in the Superseding Indictment concerning all Defendants as well as the victim ads referenced in Counts 1-51. The second DVD contained "hot docs" specifically tailored to Eisenberg's and Bertrand's individual clients. (*See* Exhibits B and C).

declaration.) The government imaged the master database servers and on March 8, 2019, provided Defendants copies of that server data (i.e. all of the ads that were on Backpage.com at the time the website was seized and shut-down). (*See* Robinson Declaration, Exhibit D, Attachment 4.) The government also imaged the image servers and on March 8, 2019, provided defendants copies of that data (i.e. all of the images that were on Backpage.com at the time the website was seized and shutdown). (*See* Robinson Declaration, Exhibit D, Attachment 4.) The government does not intend to image the replicated database servers and backup server because they are redundant to the master database servers and image servers already imaged and provided to Defendants. (*See* Robinson declaration, Exhibit D, Attachment 1.) Additionally, the government does not intend to image the various web servers because they contain no unique data. In other words, the web servers stored neither website content nor images. (*See* Robinson declaration, Exhibit D, Attachment 1.)

### B. <u>Payment Processing Island (PPI), Miscellaneous Computer Servers and CK</u>

In addition to working with W.G. to provide specific descriptions and roles of the Backpage.com website servers, the government has also worked with former Backpage.com Chief Technology Officer C.K. to provide specific descriptions and roles of servers used to house the Backpage.com Payment Processing Island (PPI), the system that received and tracked online payments for Backpage.com ads.[2] (*See* Robinson Declaration, Exhibit D and Attachments 2 and 3 to the declaration.) As mentioned above, the government will retrieve the remaining servers from Amsterdam—to include the servers that store the PPI system —the week of June 10, 2019. The government will then image the *MySQL Master Database Server* (contains all of the transaction data in the payment processing island), and the *Internal App Red Hat Web Servers* (contains web

[2] A part of C.K.'s duties as Chief Technology Officer included maintaining the servers that housed the PPI.

applications that presented data to internal Backpage employees and related companies) and make imaged copies of this server data available to Defendants on or before July 15, 2019.[3] The government does not intend to image the *MySQL Slave Database Servers* because they contain duplicate data from the *Master Database Server* and did not hold any unique data. (*See* Robinson Declaration, Exhibit D, Attachments 2 and 3.) The government also does not intend to image the *External App Red Hat Web Servers*.

In addition to the two servers seized in Dallas that contain email-related data the government made available to Defendants on March 7, 2019, the government also seized three servers in Dallas that contain backup and storage data. The government has imaged one of these servers containing various virtual machines. The other two servers are backup appliances that have not been imaged. (*See* Robinson declaration, Exhibit D ¶17, and Attachment 2, p.3.)

## III. *Jencks* Materials

The government has complied with the Scheduling Order and produced *Jencks* material in its possession (except for Carl Ferrer's *Jencks* statements) to Defendants.[4] In accordance with the Scheduling Order, if the government obtains additional *Jencks* Act material, it will disclose those materials to Defendants as soon as practicable. (*See* CR 121; p.2, footnote 3. ("If the government obtains any additional written *Jencks* material after this date [02/25/19], this *Jencks* material shall be produced promptly to the defense as soon as practicable."))

[3] This should require imaging approximately three servers. The government will provide the Court with an update regarding the imaging of this data at the June 24, 2019, status conference. The government will also notify the Court when this data has been imaged and made available to Defendants.

[4] As per the Court's April 22, 2019, Order (CR 535), the government will disclose any Jencks Act statements of Carl Ferrer on or before June 25, 2019.

## IV. Government's Proposed Dates for Extension of Existing Deadlines in the Scheduling Order

### A. Discovery and Disclosure Deadlines[5]

| | | |
|---|---|---|
| 1. | Government's rebuttal expert disclosures, if any | 09/03/2019 |
| 2. | Defendant's Production of Rule 26.2 material as to intended witnesses, if any | 07/01/2019 |

### B. Filing and Other Court Deadlines

| | | |
|---|---|---|
| 1. | Defense Disclosure of Preliminary Exhibit and Witness List | 07/01/2019[6] |
| 2. | Substantive Motions Deadline | 09/09/2019 |
| 3. | Government's Rebuttal Exhibit and Witness List | 09/09/2019 |
| 4. | Motions in Limine and Court Imposed Plea Offer expiration deadline | 10/14/2019 |
| 5. | Jury Questionnaire and Screening for Length of Trial | 11/04/2019 |
| 6. | Government's Disclosure of Final Exhibit and Witness List | 12/02/2019 |
| 7. | Defendant's Final Exhibit and Witness List | 12/09/2019 |
| 8. | Joint Voir Dire, Joint Statement of the Case, Joint Proposed Jury Instructions, Joint Proposed Verdict Form | 12/16/2019 |
| 9. | Final Pretrial Conference | 01/03/2019 at 9:00 a.m. |
| 10. | Trial | 01/15/2019 at 9:00 a.m. |

### C. Status Conferences

The parties will file a memorandum detailing the status of the case no less than seven days prior to the scheduled status conference.

| | | |
|---|---|---|
| 1. | Fourth Status Conference | 09/23/2019 at 9:00 a.m. |

[5] Although the government's initial compliance with Rule 16 discovery has passed, as noted in the existing scheduling order, if additional records are discovered by, or disclosed to the government during pretrial preparation or otherwise, pursuant to Rule 16(c), Fed. R. Crim. P., the government shall promptly disclose any additional documentary evidence or materials to the defense as soon as practicable after such disclosure or discovery occurs.

[6] The government agrees that Defendants should have the ability to supplement both their production of 26.2 materials and exhibit and witness lists after they receive the server data from the government in mid-July, but believe Defendants can make all disclosures now that are unrelated to the forthcoming server data.

Respectfully submitted this 31st day of May, 2019.

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division, U.S. Department of Justice

*s/Reginald E. Jones*
REGINALD E. JONES
Senior Trial Attorney
U.S. Department of Justice, Criminal Division
Child Exploitation and Obscenity Section

MICHAEL BAILEY
United States Attorney
District of Arizona

KEVIN M. RAPP
MARGARET PERLMETER
PETER S. KOZINETS
ANDREW C. STONE
JOHN J. KUCERA
Assistant U.S. Attorneys

# CERTIFICATE OF SERVICE

I hereby certify that on this date, May 31, 2019, I transmitted the foregoing under-seal document for filing to the Clerk of the United States District Court and sent a copy via electronic mail to: Paul J. Cambria Jr. Esq. and Erin e. McCambpell, Esq., Lipsitz Green Scime Cambria, LLC, 42 Deleware Ave, Suite 120, Buffalo, NY 14202, **pcambria@lglaw.com** and **emccampbell@lglaw.com**, Thomas H. Bienert, Jr., Esq., Whitney Bernstein, Esq., Bienart, Miller & Katzman, PLC, 903 Calle Amanecer, Suite 350, San Clemente, CA 92673, **tbisconti@bmkattorneys.com, wbernstein@bmkattorneys.com**; Jessica Ring Amunson, Jenner &block LLP, 1099 New York Ave., NW, Ste. 900, Washington DC., **jamunson@jenner.com**; Jim Grant Esq., Davis Wright Termaine, LLP, 1201 Third Avenue, Suite 2200, Seattle, WA 98101, **jimgrant@dwt.com**; Michael D. Kimerer, Esq. and Rhonda Elaine Neff, Esq., 1313 E. Osborn Road, Suite 100, Phoenix, AZ 85014, **MDK@kimerer.com** and **rneff@kimerer.com**; **david@deisenbergplc.com**, David S. Eisenberg PLC, PC, 3550 N Central Ave.,Ste. 1155,Phoenix, AZ 85012; Robert Corn-Revere Esq., Davis Wright Termaine, LLP, 1919 Pennsylvania Avenue N.W., Suite 800, Washington, D.C., 20006, **bobcornrevere@dwt.com**; Bruce Feder, Esq., 2930 East Camelback Road, Suite 160, Phoenix, AZ 85016, **bf@federlawpa.com**; Gary Linenberg, Esq., Ariel Neuman, Esq., Gopi K. Panchapakesan, Esq., Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C., 1875 Century Park East, 23rd Floor, Los Angeles, CA 90067, **glincenberg@birdmarella.com, aan@birdmarella.com, gkp@birdmarella.com.**

*s/ Angela Schuetta*
Angela Schuetta
U.S. Attorney's Office

**Exhibit A**

**From:** Jones, Reginald (CRM)
**To:** Paul Cambria; Tom Bienert; Ariel A. Neuman; Bruce Feder; Whitney Bernstein; Erin E. McCampbell (emccampbell@lglaw.com); "gpanchapakesan@birdmarella.com" (gpanchapakesan@birdmarella.com); glincenberg@birdmarella.com; "joyous@mailbag.com"; "david@deisenbergplc.com"
**Cc:** Rapp, Kevin (USAAZ); Perlmeter, Margaret (USAAZ); Kozinets, Peter (USAAZ); Stone, Andrew (USAAZ); Kucera, John (USACAC)
**Subject:** RE: Updated Exhibit List with Bates Numbers
**Date:** Wednesday, May 29, 2019 5:54:42 PM
**Attachments:** Exhibit List Updated 5.29.19.pdf

Dear Counsel:

Please find attached an updated and revised preliminary exhibit list with DOJ-BP Bates numbers for approximately 90% of the government's exhibits. We'll continue to periodically provide you with an updated and revised preliminary exhibit list in the coming weeks. (This will include adding DOJ-BP Bates numbers for the approximately 10% of documents that do not already contain a DOJ-BP Bates number.)

Additionally, approximately 20 out of the nearly 1,100 exhibits contain a Bates prefix of DOJ-AZGJ. As you are aware, documents beginning with prefix DOJ-AZGJ are documents Backpage Defendants Bates labeled and provided to us in September 2017 and we subsequently re-disclosed to you. (Backpage Defendants also previously provided these documents to the U.S. Senate Permanent Subcommittee on Investigations in 2016 as part of its investigation into Backpage.) Nevertheless, we will update the DOJ-AZGJ Bates numbered documents on the exhibit list with the corresponding DOJ-BP Bates numbers and provide the updated Bates numbers to you in the coming weeks.

Thanks,
Reggie

**Reginald E. Jones**
**U.S. Department of Justice, Criminal Division**
T: 202.616.2807 | reginald.jones4@usdoj.gov

# Exhibit B

**U.S. Department of Justice**

United States Attorney
District of Arizona

Two Renaissance Square
40 N. Central Ave., Suite 1800
Phoenix, AZ 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

May 20, 2019

Via FedEx and E-Mail
David S. Eisenberg
3550 N Central Ave., Ste. 1155
Phoenix, AZ, 85012
EMail:david@deisenbergplc.com
(attorney for Defendant Andrew Padilla)

Re: U.S. v. Michael Lacey, et al.
CR-18-00422-PHX-SMB

Dear Mr. Eisenberg:

Although we are sure you have received Mr. Piccarreta's case file regarding your client Andrew Padilla—which includes discovery disclosed in the case to date—we wanted to separately provide you two digital media devices containing "hot docs" (i.e., documents specifically related to the allegations contained in the Superseding Indictment). (*See* Superseding Indictment CR 230). DVD#1 enclosed contains approximately 1,500 pages of Bates stamped "hot docs" specifically related to the allegations in the Superseding Indictment to all Defendants as well as the victims ads referenced in Counts 1-51 of the Superseding Indictment.[1]

- *Backpage "Hot Docs"* – Bates Stamped Records DOJ-BP-0004601039-DOJ-BP-0004602110
- *Backpage Superseding Indictment "Hot Docs"* – Bates Stamped Records DOJ-BP-0004602508-DOJ-BP-0004602851

[1] Defendant Padilla is charged with Counts 1-51 of the Superseding Indictment.

- *Additional Superseding "Hot Docs"* – Bates Stamped Records DOJ-BP-0004685806-DOJ-BP-0004685877
- *Additional Victim Records* – Bates Stamped Records DOJ-BP-0004719328-DOJ-BP-0004719709

DVD#2 enclosed contains "hot docs" specifically related to allegations contained in the Superseding Indictment to Defendant Padilla. To assist your review of these materials, we have labeled each "hot doc" contained on DVD#2 (see chart below) that supports the allegations contained in the Superseding Indictment to Defendant Padilla. This allows you to cross-reference these "hot docs" with the information contained in the corresponding paragraphs of the Superseding Indictment.

| |
|---|
| SSI, paragraph 77 |
| SSI, paragraph 78 |
| SSI, paragraph 78 attachment 1 |
| SSI, paragraph 78 attachment 2 |
| SSI, paragraph 79 |
| SSI, paragraph 80 |
| SSI, paragraph 81 |
| SSI, paragraph 82 |
| SSI, paragraph 83 |
| SSI, paragraph 84 |
| SSI, paragraph 85 |
| SSI, paragraph 87 |
| SSI, paragraph 88 |
| SSI, paragraph 93 |
| SSI, paragraph 93-1 |
| SSI, paragraph 95 |
| SSI, paragraph 95 attachment |
| SSI, paragraph 96 |
| SSI, paragraph 99 |
| SSI, paragraph 99 attachment |
| SSI, paragraph 104 |
| SSI, paragraph 106 |
| SSI, paragraph 110 |
| SSI, paragraph 110 attachment |
| SSI, paragraph 116 |
| SSI, paragraph 117 |
| SSI, paragraph 117-1 |

| |
|---|
| SSI, paragraph 117-2 |
| SSI, paragraph 120 |
| SSI, paragraph 123 |
| SSI, paragraph 128 |
| SSI, paragraph 128 attachment |
| SSI, paragraph 129 |
| SSI, paragraph 132 |
| SSI, paragraph 132-1 |
| SSI, paragraph 137 |
| SSI, paragraph 145 |
| SSI, paragraph 148 |
| SSI, paragraph 149 |
| SSI, paragraph 149-1 |
| SSI, paragraph 149-2 |
| SSI, paragraph 150 |
| SSI, paragraph 150-1 |
| SSI, paragraph 150-2 |
| SSI, paragraph 150-3 |
| SSI, paragraph 150-4 |
| SSI, paragraph 150-5 |
| SSI, paragraph 150-6 |
| SSI, paragraph 150-7 |
| SSI, paragraph 150-8 |
| SSI, paragraph 150-9 |

When you have completed review of the aforementioned documents, please reach out to me with any questions.

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division
U.S. Department of Justice

*s/Reginald E. Jones*
REGINALD E. JONES
Senior Trial Attorney, CEOS
(202) 616-2807
reginald.jones4@usdoj.gov

MICHAEL BAILEY
United States Attorney

KEVIN M. RAPP
MARGARET PERLMETER
PETER S. KOZINETS
ANDREW STONE
Assistant United States Attorneys

JOHN J. KUCERA
Special Assistant U.S. Attorney

Enclosures

# Exhibit C

**U.S. Department of Justice**

United States Attorney
District of Arizona

Two Renaissance Square
40 N. Central Ave., Suite 1800
Phoenix, AZ 85004-4408

Main: (602) 514-7500
Main Fax: (602) 514-7693

May 20, 2019

Via FedEx and E-Mail
Joy Malby Bertrand
P.O. Box 2734
Scottsdale, AZ, 85252-2734
EMail:joyous@mailbag.com
(attorney for Defendant Joye
Vaught)

Re: U.S. v. Michael Lacey, et al.
CR-18-00422-PHX-SMB

Dear Ms. Bertrand:

Although we are sure you have received Mr. Weiss's case file regarding your client Joye Vaught—which includes discovery disclosed in the case to date—we wanted to separately provide you two digital media devices containing "hot docs" (i.e., documents specifically related to the allegations contained in the Superseding Indictment). (*See* Superseding Indictment CR 230). DVD#1 enclosed contains approximately 1,500 pages of Bates stamped "hot docs" specifically related to the allegations in the Superseding Indictment to all Defendants as well as the victims ads referenced in Counts 1-51 of the Superseding Indictment.[1]

- *Backpage "Hot Docs"* – Bates Stamped Records DOJ-BP-0004601039-DOJ-BP-0004602110
- *Backpage Superseding Indictment "Hot Docs"* – Bates Stamped Records DOJ-BP-0004602508-DOJ-BP-0004602851

[1] Defendant Vaught is charged with Counts 1-51 of the Superseding Indictment.

- *Additional Superseding "Hot Docs"* – Bates Stamped Records DOJ-BP-0004685806-DOJ-BP-0004685877
- *Additional Victim Records* – Bates Stamped Records DOJ-BP-0004719328-DOJ-BP-0004719709

DVD#2 enclosed contains "hot docs" specifically related to allegations contained in the Superseding Indictment to Defendant Vaught. To assist your review of these materials, we have labeled each "hot doc" contained on DVD#2 (see chart below) that supports the allegations contained in the Superseding Indictment to Defendant Vaught. This allows you to cross-reference these "hot docs" with the information contained in the corresponding paragraphs of the Superseding Indictment.

| |
|---|
| SSI, paragraph 77 |
| SSI, paragraph 78 |
| SSI, paragraph 78 attachment 1 |
| SSI, paragraph 78 attachment 2 |
| SSI, paragraph 79 |
| SSI, paragraph 93 |
| SSI, paragraph 99, part 1 |
| SSI, paragraph 99, part 2 |
| SSI, paragraph 117, part 1 |
| SSI, paragraph 117, part 2 |
| SSI, paragraph 117, part 3 |
| SSI, paragraph 128, part 1 |
| SSI, paragraph 128, part 2 |
| SSI, paragraph 129 |
| SSI, paragraph 133 |
| SSI, paragraph 137 |
| SSI, paragraph 139 |
| SSI, paragraph 143 |
| SSI, paragraph 143 attachment 1 |
| SSI, paragraph 145 |
| SSI, paragraph 148 |
| SSI, paragraph 149 |
| SSI, paragraph 157 part 1 |
| SSI, paragraph 157 part 2 |
| SSI, paragraph 185 |

When you have completed review of the aforementioned documents, please reach out to me with any questions.

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division
U.S. Department of Justice

*s/Reginald E. Jones*
REGINALD E. JONES
Senior Trial Attorney, CEOS
(202) 616-2807
reginald.jones4@usdoj.gov

MICHAEL BAILEY
United States Attorney

KEVIN M. RAPP
MARGARET PERLMETER
PETER S. KOZINETS
ANDREW STONE
Assistant United States Attorneys

JOHN J. KUCERA
Special Assistant U.S. Attorney

Enclosures

# Exhibit D

**DECLARATION OF SPECIAL AGENT RICHARD ROBINSON**

I, Special Agent Richard Robinson, declare:

**INTRODUCTION**

1. I am a Special Agent with the Internal Revenue Service Criminal Investigation (IRS-CI) and have been so employed since 2004. During my law enforcement career, I have investigated multiple violations of federal law within the jurisdiction of IRS-CI.

2. From 2004 through 2017, I was assigned to the Phoenix Field Office. My primary responsibilities there included working on white collar crime investigations including, but not limited to cases involving allegations of: bankruptcy fraud, mail fraud, wire fraud, money laundering, and income tax violations.

3. From 2017 through the present, I have worked as a Computer Investigative Specialist in the E-Crimes Section of IRS-CI. Prior to training for this position, I received my CompTIA A+ certification, which required demonstrating a basic knowledge of computer hardware and operating systems. I received six weeks of specialized training beginning in May 2017 in computer file systems and methods of acquiring, verifying and analyzing digital evidence.

4. I have participated extensively in the investigation leading up to the indictments in United States v. Michael Lacey, et al, since 2016. This declaration is submitted in support of the government's report on the status of (1) various computer servers that were used to host the Backpage.com website, (2) servers used to host a Payment Processing Island system used to receive, track and apply payments of Backpage.com and related

site users and (3) servers used to perform other functions related to Backpage.com. If called upon, I could competently testify as set forth below:

**<u>Backpage.com Website Servers, DesertNet and WG</u>**

5. Beginning on April 2018, I have corresponded with WG, the Chief Technology Officer of DesertNet regarding the computer servers that hosted the Backpage.com website. The physical computer servers that ran Backpage's website were located in Tucson and Amsterdam, as more fully described below. While the computer servers in both Tucson and Amsterdam were owned by the same ultimate business owners who owned Backpage.com, the website itself used code owned by DesertNet and DesertNet had handled the administration of the servers since Backpage.com's inception. I met WG at the Login, Inc. data center where DesertNet administered Backpage's servers in Tucson, Arizona on April 6, 2018, the day that another DesertNet employee came to the data center to shut down the servers that hosted the Backpage.com website both in Tucson and in Amsterdam. Based on all of my knowledge gathered throughout the course of this investigation, WG and his staff at DesertNet are the most knowledgeable people when it comes to the structure and operation of the Backpage.com website servers.

6. After reviewing WG's correspondence with Matt Frost of the FBI and exchanging several additional messages directly with WG, I drafted the document titled "Description and Roles of Backpage.com Website Servers" (attached as Declaration Exhibit 1) to provide a high level summary of the design of the website servers and their basic

function. WG reviewed several revisions of the document and ultimately stated that he found it consistent with his memory of how the servers were configured and operated.

7. The most relevant aspects of that summary at this time are:

A. The servers were designed to have identical data on all database servers and all image servers, so someone in possession of at least one database server and one image server would find no unique website content on any server that was not contained on those two machines. In other words, a single database server/image server pair would contain all content contained anywhere on Backpage.com.

B. No one server contains web pages as they were presented to the user when the site was active. Elements would need to be pulled from a database server and an image server for a web server to be able to generate an ad as it would have been displayed to the user.

**<u>Payment Processing Island (PPI), Miscellaneous Computer Servers and CK</u>**

8. CK served from 2015 to April 2018 as the Chief Technology Officer (CTO) for Website Technologies, LLC, a company that had the same ultimate business owners as Backpage.com and handled the operations of Backpage.com. A part of CK's duties as CTO included maintaining the servers that housed the Payment Processing Island or PPI, the Amsterdam-based system that received and tracked online payments for Backpage.com ads. While developers at Website Technologies would have handled the programming and data maintenance of different aspects of the PPI, CK had access to the administrative passwords for the system and maintained the structure that housed the system.

9. CK also administered information technology in Dallas, including offsite storage backups in Dallas and systems to store files and e-mail messages from Backpage employees. Some of these machines that housed backups had very large storage, an issue which is discussed later in this declaration. CK was the former Backpage employee who provided information about these servers as was summarized in the government's letter of March 7, 2019, and is the most knowledgeable person I know of with regard to the PPI servers and these other servers.

10. After a brief correspondence with CK, I drafted the attached document titled "Payment Processing Island Overview" (Declaration Attachment 2) to provide a high-level summary of the structure of the PPI and other related machines. This document was based in part on a diagram, also attached to this document (Declaration Attachment 3), of the PPI as it was in 2014. CK reviewed the document, proposed some changes and indicated that to his knowledge the statements are accurate and that the descriptions and functions of the machines as summarized are substantially correct.

11. The most relevant points of that summary at this time are:

A. All of the servers described are virtual machines, or VM's, meaning that they are files that run in a program on another physical server, but behave as though they were physical machines themselves.

B. Even though the location of the VM's had changed from Amazon Web Service to servers in the Switch Datacenter in Amsterdam, the basic structure and operation of the VM's remained the same as it was in 2014.

C. Once the physical machines are obtained, all of the payment data stored in the PPI will be found within the Master Database VM, which will be found on one of the physical servers. An Internal Application server VM used in connection with the Master Database VM would simplify accessing the data and likely allow running of reports from the PPI as an employee might have done prior to the PPI being shut down.

**Matthew Frost of FBI CART and Status of Receipt and Imaging[1] of Computer Data**

12. Matthew Frost is an Information Technology Specialist Forensic Examiner (ITS-FE) who has been a part of the the Computer Analysis and Response Team (CART) of the FBI for 10 years. Frost was selected for processing and analysis of the Backpage.com servers due to his specialization and experience in MySQL database systems, Linux-based servers and Z File System[2] storage. Frost has corresponded with WG and CK at various points to gain a better understanding of the servers and how to access the data on those servers.

13. In view of the high degree of redundancy built into the Backpage.com website servers, Frost has not copied the data from all of the servers because copying duplicate data would waste limited time and resources. For example:

[1] In computer forensic science, the term “image” or “forensic image” is used to describe a verifiable representation of all data stored on a given storage device. The act of acquiring such an image is referred to as imaging.

[2] A file system is a method for storing and managing digital data on storage devices, such as hard disk drives. Z File System is a relatively new file system designed with features geared to storage pools for very large amounts of data. This is not a file system that would likely be encountered on a personal computer.

A. Imaging and verifying a single terabyte (TB) of data takes about 4 hours under optimum conditions.

B. Two of the backup devices [1B35 and 1B219][3] each have at least 120 TB of storage. Frost has no devices capable of storing 120 TB of data, and no storage device capable of delivering a copy of such data to the defense. (See Declaration Attachment 4).

14. Two of the Desertnet servers from Tucson, Arizona were sent to Frost. These consisted of a Backpage.com image/picture server [1B41] and a Backpage.com master database server [1B60]. Frost imaged the two servers, and the images have been provided to the defense. (See Declaration Attachment 4).

15. Nine of the 40 Backpage.com website servers in Amsterdam were identified by WG as those that would contain data, specified as database servers, image servers and a backup server. The data from these nine servers (except for duplicate data and the backup device [1B219]) has been turned over to defense. (See Declaration Attachment 4). The other 31 website servers are expected to arrive in the U.S. in June 2019, but those servers are not expected to contain website data or images.

16. An additional five servers expected to arrive from Amsterdam this month including those that store the PPI system. CK provided a spreadsheet to Frost (and also sent a copy to me) showing the virtual servers[4] that are on those five physical servers,

[3] Numbers in square brackets and beginning with 1B refer to individual servers listed on Declaration Attachment 4.

[4] *See* Declaration Attachment 2 footnote 1 for an explanation of a Virtual Server.

approximately 26 of which appear to be related to the PPI. Based on our understanding of the PPI provided by CK (see Declaration Attachment 2), the government plans to image the servers which contain the Master Database VM and an Internal Application Server VM. The government does not plan to image other PPI servers that would contain only duplicate data or stored no transaction data.

17. Three of the servers from Dallas, Texas have been sent to Frost in Pocatello, Idaho. One of them [1B34] has been imaged, but copies of that image have not yet been provided to the defense. That server contained several VM's whose functions (as they were briefly described in the March 7, 2019 letter to the defense) included antivirus servers, asset tracking/inventory software, a backup server, a web user interface and others. According to CK the two other servers included (1) a backup appliance [1B36] with a 120 TB storage capacity used to store e-mail and subpoena data preservation requests and (2) a backup appliance [1B36] with 35 TB of storage capacity that contained copies of the Dallas office file server [1B72] and VM's hosted in the Dallas Colo [1B34] and at a facility for a company named PhoenixNAP. Neither of these last two servers has been imaged.

A. Two additional servers [1B37 and 1B72] were identified by CK as containing e-mail and documents from Backpage.com employees.

B. These two servers were imaged by a FBI CART member in Arizona and those images have been provided to defense.

18. Frost has been able to identify database entries and images that were included in ads specified in the indictment in the form of database entries and individual image files, rather than rendered as a single coherent webpage.

19. The government had hoped to preserve the servers in the Amsterdam Switch Datacenter to improve the possibility of being able to easier search and display ads as they would have appeared when the Backpage.com site was live. Dutch authorities refused to allow the servers to keep running there and indicated that they would be shut down.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge and belief. Executed this 31st day of May 2019 at Phoenix, Arizona.

Richard Robinson, Special Agent – Computer Investigative Specialist

# Attachment 1

## Description and Roles of Backpage.com Website Servers

### <u>Description of Two Data Centers</u>

The servers that stored and hosted the Backpage.com website were located both in the Switch Data Center in Amsterdam and the Login, Inc. Data Center in Tucson, Arizona.

The live data in each of these sites was synchronized and designed to be fully duplicated in each data center so that the website could maintain continuity if one data center or the other failed at any time.

When the Backpage website was seized and shut down on April 6, 2018 both the Tucson and the Amsterdam Data Centers had active servers for the Backpage.com website, broken down approximately as follows for each site:

2 Master <u>Database Servers</u>
3 (or possibly more) Replicated <u>Database Servers</u> (redundant[1] to the Master Database Servers)
3 <u>Image Servers</u> (redundant to each other)
1 Backup Server (data backups of Master <u>Database Servers</u> and <u>Image Servers</u>)
Various <u>Web Servers</u> – The remaining servers would be Web Servers or similar helper machines to help in the web serving[2] process such as load balancers[3].

### <u>Description of Three Basic Server Types</u>

The servers at both locations can be divided into three basic kinds of servers:

1. Database Servers - Contain databases for both central database and the market databases (discussed below).
    a. They do not provide any web services. They only contain the databases.
    b. These are divided into Master Database Servers and Replicated Database Servers.
        i. The master databases are the masters and where all database "writes"[4] occur.

[1] The system was designed with a great deal of redundancy in equipment and any data stored on the equipment, both for purposes of continuity (in case one or more devices should fail) and capacity/ performance (ability to provide a larger number of users with faster delivery).

[2] Web serving is delivering requested content to the user over a network.

[3] Load balancing is division of web traffic and workload between redundant machines, improving performance and reducing wear on individual machines.

[4] Writes are disk operations that result in changing of stored data.

ii. The replicated databases get near instant copies of these changes and are generally where the website "reads"[5] occur.
iii. This was simply a load balancing method to keep the web traffic on the replicated databases, which can scale, and only on the master databases when a database write needed to occur (i.e. when changes were being made).

2. Image Servers – Limited web servers used to store and serve images uploaded by users and linked to ads. The Image Servers:
   a. receive the images from advertisers,
   b. store the images on their disks,
   c. each contain a full set of the current images for the site.
   d. also serve the images. This makes them a limited web server, just images.
   e. are redundant and load-balanced.

3. Web Servers - The Web Servers dynamically generate the pages of the site and communicate with the database servers to achieve this.
   a. They are a pool of servers handling web serving for all markets including central.
   b. The Web Servers were really just the workhorses. They didn't store the content or images but they did piece it all together and dynamically generate the requested page.
   c. Said another way, Web Servers currently contain zero unique data.
   d. They do not technically serve images and instead point to the images via HTML: (<img src="">). The images are served from the image servers.
   e. The web servers are extremely redundant and load-balanced.

**<u>Overview of Basic Website Operation</u>**

All three basic server types would be involved in a typical user interaction. For example:

- A user creates an ad on an interface displayed by the Web Server, entering ad text and uploading image files to display in the ad. (1)Ad data and content are written to the Master Database Servers. (2) The images are stored on the Image Servers and (3) pointers or references to the images are written to the Database Servers and associated with the other data for that ad.

- A user clicks on a link to view an ad, causing the Web Server to generate the page by (1) reading the ad content from the Replicated Database Servers including the text of the ad, and (2) serving the page with pointers to any images referenced in the

[5] Reads are disk operations that result in accessing but not changing stored data.

database with the ad. (3) The referenced images would be served from the Image Server and appear on the page.

Because of this manner of operation, any given ad is not saved on any of the servers as a user would have seen it. Viewing a page as it would have appeared would require interaction with all three basic types of servers.

Additionally, because links and references to files and data within the servers were referenced based on the way that the servers were networked when the website was operational, restoring the website to a functional state would not necessarily be as simple as connecting any three servers of the appropriate types. Even though the any one of the Database Servers and Image Servers contain data for all Backpage.com ads at the time that the site was taken down, simulating the function of the website would require extensive time and expertise, if it is possible at all.

Enough information is available in the Database Server to determine which images were displayed with a given ad, but the processes of identifying and locating the image are not automatic.

**<u>Overview of Central Database vs. Market Databases</u>**

- The central database, called "central_backpage" included data for all users who posted ads on Backpage.com.
    - This included a portion of, but perhaps not all of, the text of any ads stored on the web servers. In the case of moderated ads, it would include the ad text, but it generally did not include all of the data.
    - This database included the filters that were applied to ads.
        - Moderation changes or actions that would apply to all ads would be applied to this database as well as the applicable market database(s).
        - While moderator action logs were generated from changes made to this table, there was no "versioning" built into the system, meaning that changed text in an ad would not have a version saved from before the change. The changed text would be the new data.
        - Images that were deleted by a moderator could remain on the Image Server and remain associated with an ad but would be flagged to not be included in an ad when the page for that ad was generated.
    - This database included a Site table that listed each market, the addresses (URLs)[6] for the market and the "jail"[7] that each market database was grouped into.

[6] Uniform Resource Locators or URLs are addresses for locating a file or resource on the Internet.

[7] The market databases were lumped into groups called "jails" to reduce the administrative and maintenance work that would otherwise need to be applied consistently to each database. Market databases could be moved between jails as needed.

- Market databases were created for each state or region and usually named after the primary city or airport, such as “nyc_backpage” or "phx_backpage" These databases are the source of the ads and will contain everything an advertiser provided for that ad, except for the actual image files, which were stored on Image Servers.
    - When a user originally posted an ad, the language and content would be saved to these databases.
    - A new/edited ad would trigger a process to copy a portion of that ad data to the central database.
        - Only the data that “central_backpage” needed was copied there.
        - For example, data such as how many bedrooms/bathrooms in a real estate ad, or the price of a bicycle for sale in a buy sell trade ad would not be copied to “central_backpage” to reduce the data flow.

# Attachment 2

# Payment Processing Island Overview

## System Overview

The attached diagram shows how the Payment Processing Island (PPI) was set up on the Amazon Web Services (AWS) network in 2014. All of the servers shown on the diagram were virtual servers[1]. In system in Amsterdam, all of the equivalent servers were also virtual servers. This was done for cost efficiency and flexibility[2] in operating and balancing the system and so that the system could be migrated, if needed.

The attached diagram is essentially how the PPI was configured in Amsterdam up through its shutdown in 2018. While the number of virtual servers on the Amsterdam servers is not the same as shown in the diagram, the functions that virtual servers perform are similar and the relationships between the virtual servers are similar.

One part missing from this diagram was the cryptocurrency portion of the system which operated in the same environment. No diagrams that would give a more current layout are readily available.

The PPI virtual machines and data were all transferred to the physical servers in the Switch Datacenter in Amsterdam. Any virtual machines or data that may have remained on AWS would not have complete sets of data, if anything was left on AWS from the old system.

## Overview of Virtual Server Types Used in the PPI

Some details of the functions of key virtual server types shown on the diagram are as follows:

***MySQL[3] Master Database Server*** (M1 on diagram) – This server housed the master database for the PPI. All transaction data, even cryptocurrency transactions, were stored in the master database on this server. Even if you had only the master database, you'd have all the transaction data in the PPI.

***MySQL Slave Database Servers*** (S1, S2, S3 on diagram) – These servers were for redundancy and reporting. They contained duplicate data from the Master Database Server, but never held any data that was not also on that server.

[1] A Virtual Server is a form of a Virtual Machine (commonly referred to as VM), which is a simulation of a whole, independent computer within another machine. Several VM's may be present in one physical server and can communicate with other VM's on the same server or other connected servers as if the VM's were physical machines connected in a network.

[2] Running servers on VM's provides cost savings in that operating several VM's often costs less than operating the same number of physical machines that would perform similar functions. VM's also provide flexibility in that a VM administrator can increase and manage the resources available to a VM (within the limits of the physical server) much more easily than upgrading a physical machine.

[3] MySQL is a commonly used open-source relational database management system.

***External App Red Hat[4] Web Server*** (W1, W2, W3, W4, W5, W6 on diagram) – These servers ran web applications that presented data in the database to external users of Backpage.com and the various affiliate websites. Payments and other changes to data made by external users would be made using online applications hosted from these servers.

***Internal App Red Hat Web Server*** (A1, A2, A3 on diagram) – These servers ran web applications used by employees of Backpage.com and related companies to access and present data in the database files for functions such as reports and research[5]. Employees used these applications to pull, review and modify transaction data.

## Overview of Data Stored in the PPI Master Database

All of the following types of transactions would have been recorded in the PPI Master Database:

- Purchases of Backpage credits that could later be used to pay for ads or ad upgrades made using:
    - Credit cards or prepaid debit cards
    - Bitcoin or other virtual currency
    - Money Orders
    - Gift cards for other businesses exchanged for credits
- Use of credits to pay for ads, ad upgrades or services such as reposting an ad.
- Direct payments using credit or debit cards or Bitcoin for ad upgrades or services
- Charges incurred on Send Me A Bill accounts (SMAB accounts) and payments made to those accounts

User payment data that was stored was limited by PCI industry guidelines[6]. For example, full credit card numbers were not stored, but rather the last four digits of the card number. Guidelines also limited the amounts and types of customers' personal identification information (such as e-mail addresses, phone numbers, etc.) data that could be stored.

Backpage.com had a policy for purging transaction data after a given time, but particular details of that policy are not readily available.

There was a way to associate ads or users with their related transactions in the PPI, but details of how that worked are not readily available.

[4] Red Hat is a variation of Linux, a type of computer operating system. (Windows and Mac OS are also types of operating systems.) The internal and external application servers in the old PPI on AWS ran using Red Hat, which is why their label on the diagram includes "Red Hat." These application servers in the PPI that was running in the Switch Datacenter in Amsterdam through April 2018 ran on another Linux variation named CentOS.

[5] While these servers do not store/house any transaction data themselves, applications on these servers would simplify accessing and interpreting the data found in the database. The applications run from the W servers and A servers are analogous to terminals that would connect to old mainframe computers, where the database acts like the mainframe, (which houses the data, but not in a user friendly format). A user who is fluent in MySQL could perform these functions without these application servers.

[6] The Payment Card Industry (PCI) Security Standards Council developed guidelines that limited the amount and types of payment and personal data that businesses were allowed store.

## Other Servers/Backup Appliances

Backup appliances located in Dallas included the following general types of data:

Backup appliance Unitrends switch Colo[7] 128 TB Storage: This was the offsite backup appliance for the Switch (PPI) environment. It should contain the same data the systems in Amsterdam did but may not include the most recent data, since backups run on a schedule instead of real time.

Backup appliance Unitrends Dallas Colo 35 TB Storage: This was the offsite backup for the Dallas office file server and PhoenixNAP[8] systems (VM's). This also contained backups of the systems (VM's) hosted at the Dallas Colo.

Synology RS18016xs+ with 120 TB storage (CARTMAN Synology NAS): This was the storage device used to store email and for email subpoena data preservation requests.

[7] Colo is a commonly used term for a colocation center, a place where several customers can have their computer servers stored and connected to the Internet, such as the Switch Datacenter in Amsterdam.

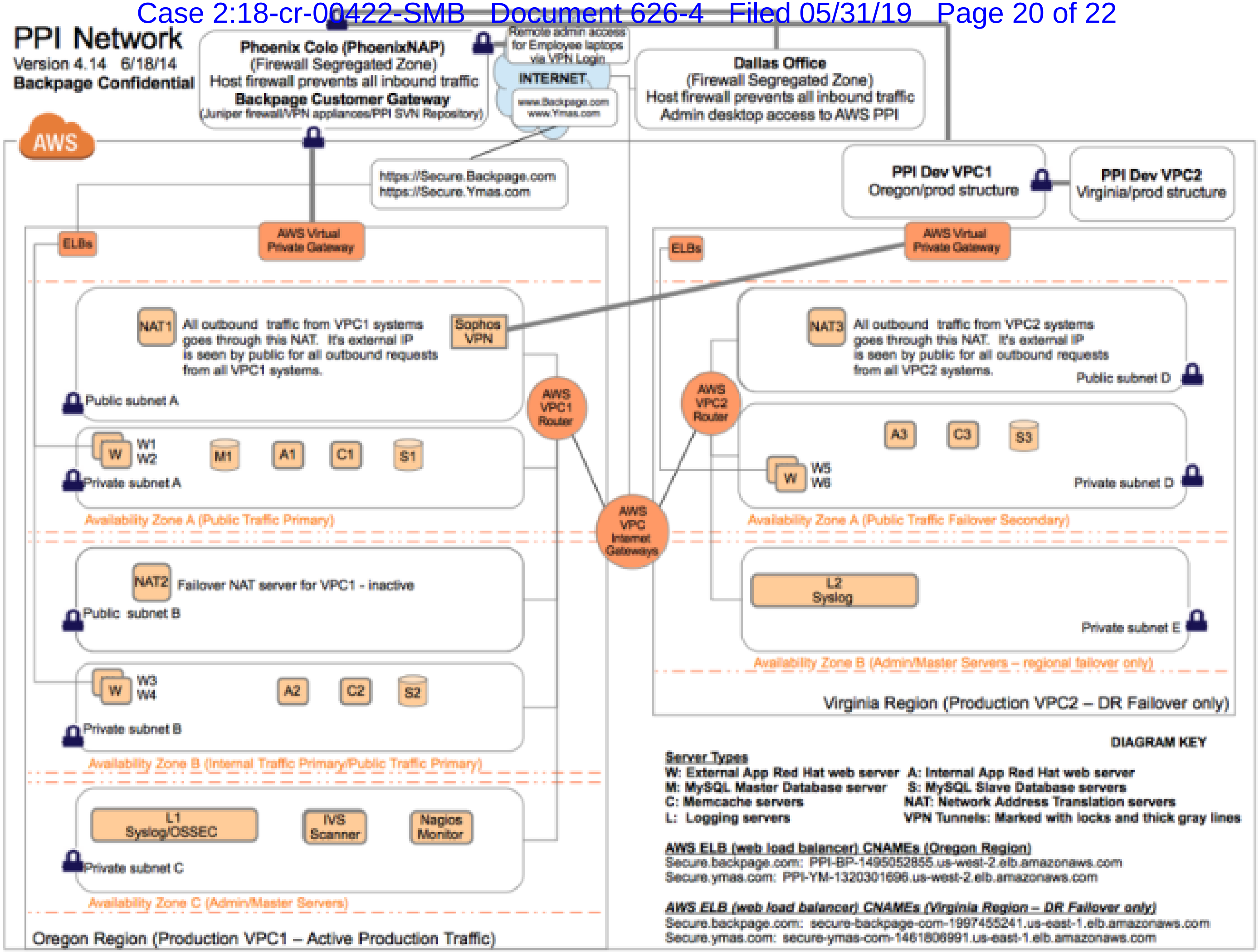
[8] PhoenixNAP is a company that offers colocation service and data hosting service.

# Attachment 3

# PPI Network

Version 4.14 6/18/14

**Backpage Confidential**



**Phoenix Colo (PhoenixNAP)**
(Firewall Segregated Zone)
Host firewall prevents all inbound traffic
**Backpage Customer Gateway**
(Juniper firewall/VPN appliances/PPI SVN Repository)

Remote admin access
for Employee laptops
via VPN Login

INTERNET

www.Backpage.com
www.Ymas.com

**Dallas Office**
(Firewall Segregated Zone)
Host firewall prevents all inbound traffic
Admin desktop access to AWS PPI

AWS

https://Secure.Backpage.com
https://Secure.Ymas.com

**PPI Dev VPC1**
Oregon/prod structure

**PPI Dev VPC2**
Virginia/prod structure

ELBs

AWS Virtual Private Gateway

NAT1 All outbound traffic from VPC1 systems goes through this NAT. It's external IP is seen by public for all outbound requests from all VPC1 systems.

Sophos VPN

Public subnet A

W W1 W2 M1 A1 C1 S1

Private subnet A

Availability Zone A (Public Traffic Primary)

AWS VPC1 Router

AWS VPC Internet Gateways

AWS VPC2 Router

NAT2 Failover NAT server for VPC1 - inactive

Public subnet B

W W3 W4 A2 C2 S2

Private subnet B

Availability Zone B (Internal Traffic Primary/Public Traffic Primary)

L1 Syslog/OSSEC

IVS Scanner

Nagios Monitor

Private subnet C

Availability Zone C (Admin/Master Servers)

Oregon Region (Production VPC1 – Active Production Traffic)

ELBs

AWS Virtual Private Gateway

NAT3 All outbound traffic from VPC2 systems goes through this NAT. It's external IP is seen by public for all outbound requests from all VPC2 systems.

Public subnet D

A3 C3 S3

W W5 W6

Private subnet D

Availability Zone A (Public Traffic Failover Secondary)

L2 Syslog

Private subnet E

Availability Zone B (Admin/Master Servers – regional failover only)

Virginia Region (Production VPC2 – DR Failover only)

**DIAGRAM KEY**

**Server Types**

**W: External App Red Hat web server** **A: Internal App Red Hat web server**
**M: MySQL Master Database server** **S: MySQL Slave Database servers**
**C: Memcache servers** **NAT: Network Address Translation servers**
**L: Logging servers** **VPN Tunnels: Marked with locks and thick gray lines**

**AWS ELB (web load balancer) CNAMEs (Oregon Region)**
Secure.backpage.com: PPI-BP-1495052855.us-west-2.elb.amazonaws.com
Secure.ymas.com: PPI-YM-1320301696.us-west-2.elb.amazonaws.com

***AWS ELB (web load balancer) CNAMEs (Virginia Region – DR Failover only)***
Secure.backpage.com: secure-backpage-com-1997455241.us-east-1.elb.amazonaws.com
Secure.ymas.com: secure-ymas-com-1461806991.us-east-1.elb.amazonaws.com

# Attachment 4

Summary of Backpage Servers Imaged/Previewed to Date

| Description of Server | Origin | Location | Type of Server | Imaged or Previewed | Raw Storage Outstanding (TB) | Provided to defense |
|---|---|---|---|---|---|---|
| 1B34 HQP002098 Dell R730xd Server (VM Server) S/N:GLF4ND2 | Dallas Colo | Pocatello | VM Server | Imaged | | No* |
| 1B35 HQP002099 Synology RS18016xs+ S/N:1650N8N101000 | Dallas Colo | Pocatello | Storage for e-mail and subpoena (120 TB) | Not imaged or previewed | 120.0 | No |
| 1B36 HQP002100 Unitrends Inc. S/N:C8260FF22N20190 | Dallas Colo | Pocatello | Dallas File Svr/PhoenixNap Backup | Not imaged or previewed | 35.0 | No |
| 1B37 (U) Dell R730xd Server S/N:7Q32GK2 | Dallas Colo | Arizona | Includes Files and e-mails | (e-mails and docs pulled)+ | | Yes |
| 1B72 (U) DELL SERVER SERIAL NUMBER 4JJSSD2 | Dallas - Backpage Office | Arizona | Includes Files and e-mails | (e-mails and docs pulled)+ | | Yes |
| 1B41 HQP001875 Dell Power Edge R720 Service Tag: 4N99H02 | Tucson | Pocatello | Image/Picture Server | Imaged | | Yes |
| 1B60 HQP001876 Dell Power Edge R920 Service Tag: 555YX12 | Tucson | Pocatello | Master Database Server | Imaged | | Yes |
| 1B211 HQP001982 Dell R730 service tag 5Z8B642 | Amsterdam | Pocatello | Master Database Server | Imaged | | Yes |
| 1B212 HQP001979 Dell R730 service tag 2Y8B642 | Amsterdam | Pocatello | Master Database Server | Imaged | | No** |
| 1B213 HQP001983 Dell R820 service tag J9SK9X1 | Amsterdam | Pocatello | Slave Database Server | Imaged | | Yes |
| 1B214 HQP001981 Dell R820 service tag 2BSK9X1 | Amsterdam | Pocatello | Slave Database Server | Previewed in Amsterdam++ | 9.7 | No |
| 1B215 HQP001980 Dell R820 service tag 1BSK9X1 | Amsterdam | Pocatello | Slave Database Server | Previewed in Amsterdam++ | 9.7 | No |
| 1B216 HQP001984 Dell R720 service tag 1FSP9X1 | Amsterdam | Pocatello | Image/Picture Server | Imaged | | Yes |
| 1B217 HQP001985 Dell R720 service tag 4FSK9X1 | Amsterdam | Pocatello | Image/Picture Server | Previewed in Amsterdam++ | 19.2 | No |
| 1B218 HQP001986 Dell R720 service tag 4FSN9X1 | Amsterdam | Pocatello | Image/Picture Server | Previewed in Amsterdam++ | 19.2 | No |
| 1B219 HQP001987 Unitrends backup-server type 938S S/N: 938S-700-70049 | Amsterdam | Pocatello | PII Backup Server | Previewed in Amsterdam++ | 128.0 | No |
| | | | | | 340.8 | |

+Frost never saw these servers but was told they were processed in Arizona

++Dutch authorities previewed these devices prior to turning them over to FBI

*Not turned over, but can be made available

**Not turned over as it was determined to be duplicate data

MICHAEL BAILEY
United States Attorney
District of Arizona

KEVIN M. RAPP (Ariz. Bar No. 14249, kevin.rapp@usdoj.gov)
MARGARET PERLMETER (Ariz. Bar No. 024805, margaret.perlmeter@usdoj.gov)
PETER S. KOZINETS (Ariz. Bar No. 019856, peter.kozinets@usdoj.gov)
ANDREW C. STONE (Ariz. Bar No. 026543, andrew.stone@usdoj.gov)
JOHN J. KUCERA (Cal. Bar No. 274184, john.kucera@usdoj.gov)
Assistant U.S. Attorneys
40 N. Central Avenue, Suite 1800
Phoenix, Arizona 85004-4408
Telephone (602) 514-7500

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division, U.S. Department of Justice

REGINALD E. JONES (Miss. Bar No. 102806, reginald.jones4@usdoj.gov)
Senior Trial Attorney, U.S. Department of Justice
Child Exploitation and Obscenity Section
950 Pennsylvania Ave N.W., Room 2116
Washington, D.C. 20530
Telephone (202) 616-2807
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

| | |
|---|---|
| United States of America,<br>Plaintiff,<br>vs.<br>Michael Lacey, et al.,<br>Defendants. | CR-18-00422-PHX-SMB<br>**NOTICE OF FILING OF GOVERNMENT'S [PROPOSED] AMENDED SCHEDULING ORDER** |

The Court has directed the parties to propose an extension of existing deadlines in the scheduling order. Accordingly, the government, through counsel undersigned, submits the following amended dates for the Court's consideration.

### A. Discovery and Disclosure Deadlines[1]

| | |
|---|---|
| 1. Government's rebuttal expert disclosures, if any | 09/03/2019 |
| 2. Defendant's Production of Rule 26.2 material as to intended witnesses, if any | 06/15/2019 |

### B. Filing and Other Court Deadlines

| | |
|---|---|
| 1. Defense Disclosure of Preliminary Exhibit and Witness List | 07/01/2019 |
| 2. Substantive Motions Deadline | 09/09/2019[2] |
| 3. Government's Rebuttal Exhibit and Witness List | 09/09/2019 |
| 4. Motions *in Limine* and Court Imposed Plea Offer expiration deadline | 10/14/2019 |
| 5. Jury Questionnaire and Screening for Length of Trial | 11/04/2019 |
| 6. Government's Disclosure of Final Exhibit and Witness List | 12/02/2019 |
| 7. Defendant's Final Exhibit and Witness List | 12/09/2019 |
| 8. Joint Voir Dire, Joint Statement of the Case, Joint Proposed Jury Instructions, Joint Proposed Verdict Form | 12/16/2019 |
| 9. Final Pretrial Conference | 01/03/2019 at 9:00 a.m. |
| 10. Trial | 01/15/2019 at 9:00 a.m. |

### C. Status Conferences

The parties will file a memorandum detailing the status of the case no less than seven days prior to the scheduled status conference.

| | |
|---|---|
| 1. Fourth Status Conference | 09/23/2019 at 9:00 a.m. |

[1] If additional records are discovered by, or disclosed to the government during pretrial preparation or otherwise, pursuant to Rule 16(c), Fed. R. Crim. P., the government shall promptly disclose any additional documentary evidence or materials to the defense as soon as practicable after such disclosure or discovery occurs.

[2] Defendants may supplement both their production of 26.2 materials and exhibit and witness lists after they receive the server data from the government in mid-July, but believe Defendants can make all disclosures now that are unrelated to the forthcoming server data.

Respectfully submitted this 31st day of May, 2019.

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division, U.S. Department of Justice

*s/ Reginald E. Jones*
REGINALD E. JONES
Senior Trial Attorney
U.S. Department of Justice, Criminal Division
Child Exploitation and Obscenity Section

MICHAEL BAILEY
United States Attorney
District of Arizona

KEVIN M. RAPP
MARGARET PERLMETER
PETER S. KOZINETS
ANDREW C. STONE
JOHN J. KUCERA
Assistant U.S. Attorneys

## CERTIFICATE OF SERVICE

I hereby certify that on this date, May 31, 2019, I transmitted the foregoing under-seal document for filing to the Clerk of the United States District Court and sent a copy via electronic mail to: Paul J. Cambria Jr. Esq. and Erin e. McCambpell, Esq., Lipsitz Green Scime Cambria, LLC, 42 Deleware Ave, Suite 120, Buffalo, NY 14202, **pcambria@lglaw.com** and **emccampbell@lglaw.com**, Thomas H. Bienert, Jr., Esq., Whitney Bernstein, Esq., Bienart, Miller & Katzman, PLC, 903 Calle Amanecer, Suite 350, San Clemente, CA 92673, **tbisconti@bmkattorneys.com, wbernstein@bmkattorneys.com**; Jessica Ring Amunson, Jenner &block LLP, 1099 New York Ave., NW, Ste. 900, Washington DC., **jamunson@jenner.com**; Jim Grant Esq., Davis Wright Termaine, LLP, 1201 Third Avenue, Suite 2200, Seattle, WA 98101, **jimgrant@dwt.com**; Michael D. Kimerer, Esq. and Rhonda Elaine Neff, Esq., 1313 E. Osborn Road, Suite 100, Phoenix, AZ 85014, **MDK@kimerer.com** and **rneff@kimerer.com**; **david@deisenbergplc.com**, David S. Eisenberg PLC, PC, 3550 N Central Ave.,Ste. 1155,Phoenix, AZ 85012; Robert Corn-Revere Esq., Davis Wright Termaine, LLP, 1919 Pennsylvania Avenue N.W., Suite 800, Washington, D.C., 20006, **bobcornrevere@dwt.com**; Bruce Feder, Esq., 2930 East Camelback Road, Suite 160, Phoenix, AZ 85016, **bf@federlawpa.com**; Gary Linenberg, Esq., Ariel Neuman, Esq., Gopi K. Panchapakesan, Esq., Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C., 1875 Century Park East, 23rd Floor, Los Angeles, CA 90067, **glincenberg@birdmarella.com, aan@birdmarella.com, gkp@birdmarella.com.**

*s/ Angela Schuetta*
Angela Schuetta
U.S. Attorney's Office